

REFERENCE TITLE: **electronic signatures; digital; technical correction**

State of Arizona  
House of Representatives  
Forty-seventh Legislature  
Second Regular Session  
2006

# **HB 2116**

Introduced by  
Representative McClure

**AN ACT**

**AMENDING SECTION 41-132, ARIZONA REVISED STATUTES; RELATING TO THE SECRETARY OF STATE AND THE DEPARTMENT OF STATE.**

(TEXT OF BILL BEGINS ON NEXT PAGE)

1 Be it enacted by the Legislature of the State of Arizona:

2 Section 1. Section 41-132, Arizona Revised Statutes, is amended to  
3 read:

4 41-132. Electronic and digital signatures: exemptions:  
5 definitions

6 A. Unless otherwise provided by law, an electronic signature that  
7 complies with this section may be used to sign a writing on a document that  
8 is filed with or by a state agency, board or commission and the electronic  
9 signature has the same force and effect as a written signature.

10 B. An electronic signature shall be unique to the person using it,  
11 shall be capable of reliable verification and shall be linked to a record in  
12 a manner so that if the record is changed the electronic signature is  
13 invalidated.

14 C. A document that contains an electronic signature that is a digital  
15 signature shall comply with all of the following:

16 1. Contain a computer based certificate that identifies the issuing  
17 entity and the subscriber, contain the subscriber's public key and be  
18 digitally signed by the issuing entity. A valid subscriber to a digitally  
19 signed document shall be listed in the certificate, shall accept the  
20 certificate and lawfully holds the private key that corresponds to the public  
21 key that is listed in that certificate. A person who acquires a private key  
22 through theft, fraud, deceit, eavesdropping or other unlawful means does not  
23 lawfully hold the private key.

24 2. Contain a key pair used for verifying a digital signature that has  
25 a unique property so that the public key can verify the digital signature  
26 that the private key creates.

27 3. Be capable of verification by the person having the initial message  
28 and the signer's public key as follows:

29 (a) The person can accurately determine whether the transformation of  
30 the message was created by using the private key that corresponds to the  
31 signer's key.

32 (b) The person can accurately determine whether the initial message  
33 has been altered since the transformation was made.

34 D. The following records are not public records and are exempt from  
35 public inspection and reproduction pursuant to title 39, chapter 1,  
36 article 2:

37 1. Records containing information that would disclose or may  
38 reasonably lead to the disclosure of any component in the process used to  
39 execute or adopt an electronic or digital signature if the disclosure would  
40 or may reasonably cause the loss of sole control over the electronic or  
41 digital signature from the person using it.

42 2. Records that if disclosed would **JEOPARDIZE** or may reasonably lead  
43 to jeopardizing the security of a certificate issued in conjunction with a  
44 digital signature.

- 1           E. In this section, unless the context otherwise requires:
- 2           1. "Asymmetric cryptosystem" means an algorithm or series of
- 3 algorithms that provide a secure key pair for a digital signature.
- 4           2. "Certificate" means a computer based record that is contained in a
- 5 document with a digital signature and that identifies the subscriber,
- 6 contains the subscriber's public key and is digitally signed by the entity
- 7 issuing the certificate.
- 8           3. "Digital signature" means a type of electronic signature that
- 9 transforms a message through the use of an asymmetric cryptosystem.
- 10          4. "Electronic signature" means an electronic or digital method of
- 11 identification that is executed or adopted by a person with the intent to be
- 12 bound by or to authenticate a record.
- 13          5. "Entity issuing a certificate" means a person who creates and
- 14 issues a certificate and notifies the subscriber listed in the certificate of
- 15 the contents of the certificate.
- 16          6. "Key pair" means a private key and its corresponding public key in
- 17 an asymmetric cryptosystem.
- 18          7. "Person" means a human being or an organization capable of signing
- 19 a document, either legally or as a matter of fact.
- 20          8. "Private key" means the key of a key pair that is used to create a
- 21 digital signature.
- 22          9. "Public key" means the key of a key pair that is used to verify a
- 23 digital signature.
- 24          10. "Record" means information that is inscribed in a tangible medium
- 25 or that is stored in an electronic or other medium and that is retrievable in
- 26 a physically perceivable form. Record includes electronic records and
- 27 printed, typewritten and tangible records.
- 28          11. "Subscriber" means a person who is the subject listed in a
- 29 certificate, accepts that certificate and holds a private key that
- 30 corresponds to a public key listed in that certificate.
- 31          12. "Transform" or "transform a message" means to subject data in a
- 32 message to a mathematical change by electronic means.